ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC. TYPE:	Liaison Statement
TITLE:	Liaison Statement from the Common Criteria Interpretations Management Board (CCIMB) to ISO/IEC JTC 1/SC 27/WG 3 in response to document SC 27 N 2285 (WG 3 N474)
SOURCE:	CCIMB Liaison Officer (U. van Essen)
DATE:	1999-09-30
PROJECT:	1.27.16
STATUS:	This document is being submitted for consideration at the next SC 27/WG 3 and SC 27 Plenary meetings in Columbia, MD, U.S.A., October 4 - 13, 1999.
ACTION:	**ACT**
DUE DATE:	1999-10-04
DISTRIBUTION:	P, O and L-Members W. Fumy, SC 27 Chairman M. De Soete, T. Humphreys, S. Knapskog, WG-Conveners U. van Essen, SC 27 Liaison Officer
MEDIUM:	Server
NO. OF PAGES:	6

ISO - International Organisation for Standardisation
IEC - International Electrotechnical Commission

JTC 1 - „Information Technology"
SC 27 - „Security Techniques"
WG 3 - „Security Evaluation Criteria"

TITLE: CCIMB Liaison Statement to ISO/IEC JTC1/SC 27/WG 3
            (CCIMB-99-040)
SOURCE: CCIMB Liaison Officer, Ulrich van Essen

DATE: 1999-09-29

PROJECT: JTC 1.27.16

STATUS: For study by JTC 1/SC 27/WG 3 experts

COMMON CRITERIA INTERPRETATIONS MANAGEMENT BOARD
Liaison Statement to ISO/SC27/WG3
1999-09-29

Introduction

This liaison statement from the Common Criteria Interpretations Management Board (CCIMB) provides a response to the ISO WG3 liaison statement to the CCIMB from the April 1999 WG3 meeting in Madrid/ Spain (WG3 N474). Due to the fact that a CCIMB meeting took place in the week before the October 1999 WG 3 meeting, this liaison statement could only be e-mailed to WG3 experts a few days before the meeting.

The CCIMB thanks ISO/SC27/WG3 for the proposals and contributions made in the document N474.

1. Publication of a Version 2.1 of the Common Criteria (CC)

As the ballot on the Final Draft International Standard 15408 ended in June 1999 with the excellent result of 29 approvals, 2 abstentions and no disapprovals, the CC project decided in the interest of as much coincidence with the International Standard ISO/IEC 15408 as possible to publish a version 2.1 of the Common Criteria. It contains all the ISO initiated changes to the document, which were made after WG 3 and the former CCIB agreed on a common version on the occasion of the April 1998 joined meeting in Stockholm, Sweden. That version was then published as CC version 2.0 in May 1998.

Together with version 2.1 of the CC the CC project will publish a document identifying noteworthy changes between CC version 2.0 and version 2.1.

The only textual difference between the IS 15408, which still awaits publication, and the CC is that all direct characterisations of the International Standard, namely title, foreword and text mentioning "ISO/IEC 15408", have been replaced by CC wording. Thus the two documents are technically identical, and evaluations based on the one document can claim to fulfil also the requirements of the other. On the other hand it is made clear that the International Standard is solely published by ISO/IEC and its national bodies.

2. Criteria Maintenance
The Common Criteria Project is beginning its maintenance activities of the Common Criteria. The CCIMB has been charged by the Project to perform this maintenance. To this end, the CCIMB has created an intepretation/revision process which is summarised in the document entitled *CC Maintenance Overview* (CCIMB-99-039). The CCIMB will be pleased to discuss any questions concerning support in maintaining ISO/IEC 15408 with ISO bodies (e.g., JTC1/SC27/WG3). The ongoing intent is to co-operate with ISO to best ensure the common needs of the CC project and ISO are met.

3. Common Methodology for IT Security Evaluation (CEM)

The CC projects thanks for the contributions made for the CEM development which have been provided in the liaison statement N474. Several Common Evaluation Methodology Observation Reports (CEMORs) have been generated as an impact of those comments and have been addressed alongside of the public review in the production of version 1.0. On the occasion of the upcoming WG 3 meeting the CC project will summarise the handling of the more than one thousand CEMORs received.

Version 1.0 of the CEM is finalised in October 1999 and will subsequently be published on several of the CC project organisation's websites. It contains evaluation methods for TOE evaluations up to EAL 4 and for PP and ST evaluations.

The CEM is now practically applied. In parallel, the Common Evaluation Methodology Editorial Board continues to develop evaluation methods including consideration of assurance maintenance and flaw remediation.

4. Translations of the criteria

A draft version of the German translation of the CC version 2.0 has been published at the BSI's website (www.bsi.de/cc). A French translation of Part 1 of version 2.0 has been handed over to the French Standardisation Body AFNOR.

Common Criteria Interpretations Management Board

CCIMB

CC Maintenance Overview

Author(s)   U. van Essen/R. Harland

Summary

This document summarises CC maintenance activities by the Common Criteria Interpretations Management Board.

1   Need for maintenance

1   In order to adequately monitor compliance of security evaluations to the CC, national schemes with certification/validation bodies are necessary in order to ensure that these evaluations are as objective as possible. This is especially important, given that mutual recognition arrangements are already in place to ensure that a certain IT product or system only needs to be evaluated once, with the results of that evaluation being broadly recognised in many different countries.

2   To support mutual recognition of evaluation results, the CC must be applied within the national schemes in a consistent manner. As a direct result, there is the need for regular, timely harmonised interpretations of the criteria to ensure that they are being used in a appropriate manner for each of the many different types of applications. These interpretations will be a valuable input to the maintenance of the CC, because they represent experience from its practical application.

2   Maintenance activities

3   In its role as the CC project's maintenance body, the CCIMB analyses all Requests for Interpretations (RIs) including:

  a)   questions on the application of the criteria,

  b)   perceived editorial and technical errors, and

  c)   statements on appropriate requirements in areas currently not covered in the CC.

4   Sources of RIs include users of the CC from around the world. However, it is expected that most RIs will arise from formal evaluations performed under the national schemes that are part of mutual recognition arrangements (MRA). The CCIMB will prioritise the RIs and respond to each, in priority order. A response will be issued to the originator of the request and, if appropriate, posted to the Internet for public review. After the public review, the CCIMB will review any feedback and finalise the interpretation (with adjustments if appropriate) . Final interpretations agreed by the CCIMB will be considered to be part of the CC, and will be levied on all subsequent evaluations certified by organisations party to the MRA.

5   Periodically, revised versions of the CC will be published, depending on the number and nature of the finalised interpretations.